



DEPARTMENT OF THE ARMY
US ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, UNITED STATES ARMY GARRISON, FT MONROE
102 MCNAIR DRIVE
FORT MONROE VIRGINIA 23651-1047

REPLY TO
ATTENTION OF

Expires: 16 April 2009

IMNE-MNR-IM

16 April 2007

MEMORANDUM FOR Directors and Office Chiefs, HQ Fort Monroe

SUBJECT: Fort Monroe Policy Memorandum #2, Data-At-Rest (DAR)
Protection for Mobile Computing Devices (MCDs)

1. References.

a. Memorandum, Chief Information Officer (CIO)/G-6
(SAIS-GKP), 28 Sep 06, subject: Army Data-At-Rest (DAR)
Protection Strategy.

b. Army Best Business Practice (BBP), Data-At-Rest (DAR)
Protection, Mobile Devices using Encrypting File System (EFS)
Implementation, 12 Oct 06.

2. Background. The Army continues to lose sensitive information due to negligence in protecting data on MCDs and removable media. These losses place the lives of Soldiers at risk. Therefore, the Army has set forth requirements for encrypting information on all MCDs and removable storage devices. MCDs are defined as laptops, tablet-PCs, portable notebooks, USB hard drives, USB thumb drives, and similar systems.

3. Applicability. This policy memorandum applies to the Garrison, Fort Monroe.

4. Responsibilities. Commanders/Directors, Information Management Officers (IMOs), and Information Assurance Security Officers (IASOs) must be proactive in ensuring users are trained on DAR policies. Mobile devices must be configured for protection from existing and emerging threats by ensuring the following actions are implemented:

a. Ensure all assigned mobile information systems (IS) have DAR software installed that has been approved for travel off Department of Defense (DoD) installations or out of government-controlled facilities not located on an installation.

IMNE-MNR-IM

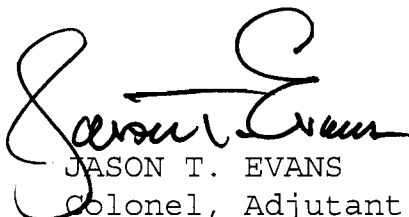
SUBJECT: Fort Monroe Policy Memorandum #2, Data-At-Rest (DAR)
Protection for Mobile Computing Devices (MCDs)

b. Implement local procedures to identify, label and account for MCDs and removable media as directed. Labeling should indicate compliance with this policy.

c. Limit the amount of sensitive information that is transported out of facilities on MCDs, hard drives, thumb drives, or any removable media to the minimum necessary to accomplish mission objectives.

d. Ensure the importance of safeguarding information on MCDs and removable media is emphasized during initial and annual IS user training.

5. Point of contact is Mr. Garland Henley, Installation Information Assurance Manager, at telephone number (757) 788-2690.

A handwritten signature in black ink, appearing to read "Jason T. Evans". The signature is stylized with a large, looping "J" and "E".

JASON T. EVANS
Colonel, Adjutant General
Commanding